CLAIMS

What is claimed is:

1. A method comprising:

generating a first key;

generating first validity data based on first backup data and the first key;

sending the first key to a peer storing the first backup data; and

requesting second validity data from the peer to determine whether the first backup data is preserved by the peer, wherein the second validity data is based on the first backup data stored by the peer and the first key.

2. The method of claim 1, further comprising:

penalizing the peer if the second validity data is not timely received from the peer.

3. The method of claim 2, further comprising:

receiving the second validity data from the peer;

determining whether the first validity data and the second validity data are different; and

penalizing the peer if the first validity data and the second validity data are determined to be different.

4. The method of claim 3, further comprising:

storing second backup data received from the peer, wherein penalizing the peer comprises deleting the second backup data.

5. The method of claim 3, further comprising:

providing the peer with consideration for storing first backup data, wherein penalizing the peer comprises recovering at least a portion of the consideration.

6. The method of claim 1, wherein the first backup data is encrypted.

7. The method of claim 1, wherein generating first validity data comprises:

combining the first key and the first backup data to create first keyed backup data; and

performing a one-way hash function on the first keyed backup data.

8. The method of claim 7, wherein the one-way hash function is selected from the group consisting of MD5, SHA-1, and RIPEMD-160.

9. The method of claim 1, further comprising:

generating a plurality of additional keys;

generating additional validity data for each of the additional keys, wherein each additional validity data is based on the first backup data and one of the additional keys;

sending a selected one of the additional keys to the peer; and

requesting third validity data from the peer to determine whether the first backup data is preserved by the peer, wherein the third validity data is based on the first backup data stored by the peer and the selected one of additional keys.

10. The method of claim 9, further comprising:

storing the additional validity data and the additional keys.

11. An article of manufacture comprising:

a machine-accessible medium including data that, when accessed by a machine, cause the machine to perform operations comprising:

generating a first key;

generating first validity data based on first backup data and the first key;

sending the first key to a peer storing the first backup data; and

requesting second validity data from the peer to determine whether the first backup data is preserved by the peer, wherein the second validity data is based on the first backup data stored by the peer and the first key.

12. The article of manufacture of claim 11, wherein the machine-accessible medium further includes data that cause the machine to perform operations comprising:

penalizing the peer if the second validity data is not timely received from the peer.

13. The article of manufacture of claim 12, wherein the machine-accessible medium further includes data that cause the machine to perform operations comprising:

receiving the second validity data from the peer;

determining whether the first validity data and the second validity data are different; and

penalizing the peer if the first validity data and the second validity data are determined to be different.

14. The article of manufacture of claim 13, wherein the machine-accessible medium further includes data that cause the machine to perform operations comprising:

storing second backup data received from the peer, wherein penalizing the peer comprises deleting the second backup data.

15. The article of manufacture of claim 13, wherein the machine-accessible medium further includes data that cause the machine to perform operations comprising:

providing the peer with consideration for storing first backup data, wherein penalizing the peer comprises recovering at least a portion of the consideration.

16. The article of manufacture of claim 11, wherein the first backup data is encrypted.

17. The article of manufacture of claim 11, wherein generating first validity data comprises:

combining the first key and the first backup data to create first keyed backup data; and

performing a one-way hash function on the first keyed backup data.

18. The article of manufacture of claim 17, wherein the one-way hash function is selected from the group consisting of MD5, SHA-1, and RIPEMD-160.

19. The article of manufacture of claim 11, wherein the machine-accessible medium further includes data that cause the machine to perform operations comprising:

generating a plurality of additional keys;

generating additional validity data for each of the additional keys, wherein each additional validity data is based on the first backup data and one of the additional keys;

sending a selected one of the additional keys to the peer; and

requesting third validity data from the peer to determine whether the first backup data is preserved by the peer, wherein the third validity data is based on the first backup data stored by the peer and the selected one of additional keys.

20. The article of manufacture of claim 19, wherein the method further comprises:

storing the additional validity data and the additional keys.

21. A system for validating first backup data, the system comprising:

a twisted pair cable;

a data storage device;

a key generator to generate a first key;

a validity data generator to generate first validity data based on the first backup data and the first key;

a communication device to send the key to a peer storing the first backup data and to request second validity data from the peer, wherein the second validity data is based on the first backup data stored by the peer and the first key; and

a validity data comparator to determine whether the first backup data is preserved by the peer.

22. The system of claim 21, further comprising:

the communication device to receive the second validity data from the peer; and

a penalty generator to inflict a penalty against the peer if the second validity data is not timely received from the peer.

23. The system of claim 22, further comprising:

the validity data comparator to compare the first validity data and the second validity data; and

the penalty generator to inflict a penalty against the peer if the first validity data and the second validity data do not match.

24. The system of claim 23, wherein the penalty comprises deletion of second backup data received from the peer.

25. The system of claim 23, wherein the penalty comprises recovering a portion of consideration provided to the peer for storing the first backup data.

26. The system of claim 21, wherein the first backup data is encrypted.

27. The system of claim 21, further comprising:

the validity data generator to combine the first key and the first backup data to create first keyed backup data and to perform a one-way hash function on the first keyed backup data.

28. The system of claim 27, wherein the one-way hash function is selected from the group consisting of MD5, SHA-1, and RIPEMD-160.

29. The system of claim 21, further comprising:

the key generator to generate a plurality of additional keys;

the validity data generator to generate additional validity data for each of the additional keys, wherein each additional validity data is based on the first backup data and one of the additional keys;

the communication device to send a selected one of the additional keys to the peer and to request third validity data from the peer; and

the validity data comparator to determine whether the first backup data is preserved by the peer, wherein the third validity data is based on the first backup data stored by the peer and the selected one of additional keys.

30. The system of claim 29, further comprising:

the data storage device to store the additional validity data and the additional keys.